



Marshall Space Flight Center

HOSC Two Factor Authentication Update Presentation to CSA TIM Oct 2012



Approved for Public Release; Distribution Unlimited.



Marshall Space Flight Center

Two Factor Authentication Update to CSA TIM 10-16-12

Purpose:

Satisfy United States Homeland Security Presidential Directive-12

“KNOW WHO YOUR USERS ARE”

Scope:

How? **TWO FACTOR AUTHENTICATION**

Two factors are:

- something you know
- something that is unique to you.

HOSC Method:

NASA Agency issued RSA Token and User provided PIN

Implementation:

Operational

- POIF Cadre - Completed
- New Customers – As Manifested.
- Existing Customers.– Process has begun. Payloads notified before we begin.

Systems affected:

Enhanced HOSC Systems Services (EHS Programmatic Command/Telemetry Services)
Enhanced HOSC Systems EHS Web Services (PIMS, NRT, etc.)
Payload Planning systems (PPS/URC)
Remote IVoDS, and HOSC OSTPV/iPV
HOSC Firewall VPN

Two Factor Authentication Update to CSA TIM 10-16-12

Process

1. Payloads identify users in Ground Data Services (GDS) Blank Book
 - a. Initial user base to include user's ground support personnel access if required.
 - b. Update user base
 - (1) Add new users
 - (2) Delete terminated user.
2. HOSC submits a MSFC affiliation request in NASA's IdMAX system so we can get a NASA Agency Identity (AUID) for the user.
3. Once HOSC submits, IdMAX MSFC affiliation request, IdMAX sends e-mail to individual, assuming he/she gave us good e-mail, and that person has three days to respond to the request for personal information. If they do not, then we have to go back to step 2 again.
4. Once step 2 is completed, we have to wait on the Agency to do a background check on the individual. Can take up to two weeks and sometime longer.
5. Once background is done, the user is notified to register and take NASA's on line IT Security Training.
 - If user unable to access NASA SATERN system to take annual training then HOSC provides training package and user training compliance letter .
 - User reviews training material, signs training compliance letter and returns letter to HOSC.

Two Factor Authentication Update to CSA TIM 10-16-12

Process Continued

6. Once IT Security Training is done the HOSC proceeds to provision the accounts .
 - A. The user requests in IdMAX a “HOSC ISS Remote Payload User” account.
 - B. If user can’t access IdMAX the the HOSC makes for them in IdMAX.
 - C. This IdMAX process includes a request for an Agency issued RSA Token.
 - D. Once approved in IdMAX (usually no more than 1 to 2 weeks) the HOSC starts creating the accounts.
 - E. The user, if located at a NASA Center is requested to pick up his/her RSA Token.
 - F. The user, if not located at a NASA Center is mailed the RSA Token.
7. Once accounts are created and RSA Tokens has been received, the user is notified that requested accounts are enabled for use via e-mail.

THIS PROCESS CAN TAKE ANYWHERE FROM 2 WEEKS TO 2 MONTHS DEPENDING ON USER RESPONSE TO REQUEST AND RSA TOKEN DISTRIBUTION PROCESS